Atari Online News, Etc.
A-ONE Online Magazine
Dana P. Jacobson, Publisher/Managing Editor
Joseph Mirando, Managing Editor
Rob Mahlert, Associate Editor

Atari Online News, Etc. Staff

Dana P. Jacobson -- Editor
Joe Mirando -- "People Are Talking"
Michael Burkley -- "Unabashed Atariophile"
Albert Dayes -- "CC: Classic Chips"
Rob Mahlert -- Web site
Thomas J. Andrews -- "Keeper of the Flame"

With Contributions by:

Fed Horvat

To subscribe to A-ONE, change e-mail addresses, or unsubscribe,
log on to our website at: www.atarinews.org
and click on "Subscriptions".
OR subscribe to A-ONE by sending a message to: dpj@atarinews.org
and your address will be added to the distribution list.
To unsubscribe from A-ONE, send the following: Unsubscribe A-ONE
Please make sure that you include the same address that you used to
subscribe from.

To download A-ONE, set your browser bookmarks to one of the
following sites:

http://people.delphiforums.com/dpj/a-one.htm
Now available:
http://www.atarinews.org

Visit the Atari Advantage Forum on Delphi!
http://forums.delphiforums.com/atari/

=~=~=~=

A-ONE #1806 02/12/16

~ Obama: Passwords, Plus! ~ Bye, Bye Adobe Flash! ~ Malware Museum Open!

-* Doom Collector's Edition News *-
-* Harvard Debunks "Going Dark" Claim! *-
-* Twitter Suspends Terrorist Content Accounts *-

=~=~=~=

->From the Editor's Keyboard "Saying it like it is!"
""""""""""""""""""""""""""""

I apologize for last week, but we just didn't have enough material to warrant putting out an issue. So, here we are this week with plenty of news that should keep you busy for awhile!

We've finaly experienced winter this past week! A couple of small storms hit the Northeast, but really didn't amount to a lot of snow. In fact, I didn't even bother to fireup the snow thrower to clean it up. It has been, however, brutally cold lately, with the worst to come this weekend as we reach sub-zero temperatures! I don't even think that the dogs are going to want to stay out in that kind of weather either! On the positive side, early forecasts call for a couple of days next week with temps close to the 50-degree mark. That kind of weather I can handle just fine!

So, bundle up near the fire or under your blankets and enjoy this week's issue of A-ONE; we're a cold weather beater!

Until next time...

=~=~=~=

FireBee Update News

By Fred Horvat

It s been a busy couple of weeks that I have not had any hands on time with the FireBee. I did figure out something with my FireBee not booting properly. Most of the time when it does not cold boot the Date and Time are set back to 08-01-2010. I did a post of the issue on Atari-Forum.com http://www.atari-forum.com/viewtopic.php?f=92&t=29237 There were other users having the exact same issue as me. A small number of FireBee owners (myself included) started having this issue after we upgraded our BaS (BasicSystem) Firmware. The solution is to reflash the BaS to the original CodeWarrior Version located here: http://firebee.org/~firebee/pictures/files/BaS-20120613.zip I have not had time to do this yet but it is next on my list with

the FireBee.

Also I did a little more reading on Atari FreeMiNT and what it would take to install SpareMiNT to the FireBee. I came across an old Web Page that explains really well how all the pieces of MiNT are put together on an Atari Computer. The software and versions are out dated but I feel it is well written. The Web Page is here: http://www2.gol.com/users/oskelton/mint.html Another Web page I came across that went into FreeMiNT and other pieces of the Atari Operating System that I thought explained things well was at http://ae.dhs.nu/krapmint/aaargh.txt

Lastly also while researching I came back across something I read last Summer but forgot about. This is MyAES http://myaes.lutece.net/ The AES is defined as The AES is responsible for window and menu control, messaging services, and object rendering and manipulation. The AES under FireBee FreeMiNT is XaAES which to me works really well. But since the pieces of the operating system are modular I can replace XaAES with MyAES and see how the Windowing looks and behaves with MyAES. MyAES has very positive comments and reviews. Something else to try out in the future, after backing up first of course

Maggie 25th Anniversary

Fifteen years after the last one, most of which time has been spent screaming "Noooo, never again!" by me, the Maggie Team are proud to present an extra special 25th anniversary commemorative issue of the legendary Maggie disk-mag.

It’s available in a HTML fake-menu format with lots of pictures, as beloved by almost no-one. Better still, there is also a proper old school Atari ST Maggie diskmag with the traditional menu shell. Like we used to make in the good old days. A disk image is supplied, if you want to copy it around, use 80 tracks and 10 sectors for your real or pretend floppy disk. It can live on a hard disk. It is using quite an old version of the shell, so probably not Falcon compatible.

As for what’s inside, we’ve tried to cover as much of the last two years as we could, full reports on the Outline and STNICCC Parties are in there, the summer highlights of Sommerhack, a comprehensive history of Maggie from issue one, news and reviews and much much more, as they say.

Is this a one-off? Probably not, but don’t hold your breath. At least it won’t be so long for the next time.

Anyway, enough from me, download, read, enjoy!

http://demozoo.org/productions/152817/

Or the HTML edition from here:

http://files.dhs.nu/files_magazines/maggie25.th/magfront.htm

=~=~=~=

->In This Week’s Gaming Section - Doom Release Date, $120 Collector’s Edition Announced!
"""""""""""""""""""""""""""""""

=~=~=~=

->A-ONE’s Game Console Industry News - The Latest Gaming News!
"""""""""""""""""""""""""""""""""""""

Doom Release Date, $120 Collector’s Edition Announced

Bethesda announced that id Software’s long-in-development new Doom game will launch globally on May 13. It will arrive on that date for PlayStation 4, Xbox One, and PC. A new trailer was also released.

You won’t have to wait that long to play the game, as a beta will be held before launch. However, there is no word yet on when this will begin. Asked to provide an update on the beta, a Bethesda representative told GameSpot that details will be announced at a later date.

The publisher also has announced a Doom collector’s edition, the centerpiece of which is a 12" statue of one of the game’s baddest demons: the Revenant. The figure was made by TriForce, which used actual game files from id Software to nail the creature’s look. The beast stands on an LED-lit base and should frighten anyone who comes by your desk.

NVIDIA slashes the prices on a selection of critically acclaimed games available on SHIELD worth playing this winter.

Doom’s collector’s edition, which will sell for $120, also comes with a copy of the game in a metal case.

Bethesda also today announced preorder bonuses for Doom. Everyone who preorders the shooter gets the Demon Multiplayer Pack. This comes with a demon armor set, which itself features three skin variations, six paint colors, and three id Software patterns to put on your armor and weapons. It also packs in six "Hack Modules," consumable items that can be used in game to give you an edge in the arena.

It’s been a long time coming for Doom. Following a failed first attempt at designing a Call of Duty-inspired Doom reboot, Bethesda restarted the project with more of a traditional concept at its

core.

=~=~=~=

A-ONE’s Headline News
The Latest in Computer Technology News
Compiled by: Dana P. Jacobson

Harvard Report Debunks Government’s ’Going Dark’ Encryption Claim

Federal investigative agencies like the FBI have long argued that encryption and other new technologies severely hamper their ability to spy on terrorists and other criminals, putting our safety at risk. A new report from Harvard debunks that "going dark" claim, concluding that the rise of network-connected devices will lead to more, not fewer, opportunities for surveillance.

Harvard’s Berkman Center for Internet & Society convened a group of security and policy experts to explore questions of surveillance and encryption at a time when major tech companies like Apple and Google are encrypting their phones and other products by default. The 37-page report, released Monday, concludes that the feds’ "going dark" argument falls flat on its face.

"Are we really headed to a future in which our ability to effectively surveil criminals and bad actors is impossible? We think not," the report says.

FBI Director James Comey, in an October 2014 speech, argued that the law hasn’t kept pace with technologies, like encryption, that have become "the tool of choice for some very dangerous people."

"We call it ’Going Dark,’ and what it means is this: Those charged with protecting our people aren’t always able to access the evidence we need to prosecute crime and prevent terrorism even with lawful authority," Comey said. "We have the legal authority to intercept and access communications and information pursuant to court order, but we often lack the technical ability to do so."

But the Berkman Center report says it’s unlikely that companies will ubiquitously adopt end-to-end encryption, because many of them rely on access to user data for revenue streams and product functionality. Furthermore, there is no industry standard for encryption.

The report also says the rise of connected devices and the Internet of Things offers new opportunities for surveillance. "The still images, video, and audio captured by these devices may enable real-time intercept and recording with after-the-fact access," the report states.

The report concludes that the "going dark" metaphor isn’t an accurate description of the future of the government’s ability to intercept the communications of suspected criminals.

"The increased availability of encryption technologies certainly impedes government surveillance under certain circumstances, and in this sense, the government is losing some surveillance opportunities," the panel said. "However, we concluded that the combination of technological developments and market forces is likely to fill some of these gaps and, more broadly, to ensure that the government will gain new opportunities to gather critical information."

Twitter Suspends 125,000 Accounts in ’Terrorist Content’ Crackdown

Twitter suspended over 125,000 accounts, most of them linked to the Islamic State group, as part of a stepped-up effort to eradicate "terrorist content" on the popular messaging platform, it said Friday.

The accounts frozen since mid-2015 were targeted "for threatening or promoting terrorist acts," said Twitter, which is under pressure from governments to act but faces a delicate balancing act and is keen not to be seen to be effectively censoring free speech.

"Like most people around the world, we are horrified by the atrocities perpetrated by extremist groups," Twitter said on its policy blog.

"We condemn the use of Twitter to promote terrorism and the Twitter rules make it clear that this type of behavior, or any violent threat, is not permitted on our service."

The announcement comes after the United States and other governments urged social networks to take more aggressive steps to root out activity aimed at recruiting and planning violent acts.

Twitter said it already has rules to discourage this activity but that it was driving up enforcement by boosting staff and using technology to filter violence-promoting content. But it warned there is no easy technological solution.

"As many experts and other companies have noted, there is no ’magic algorithm’ for identifying terrorist content on the Internet, so global online platforms are forced to make challenging judgment calls based on very limited information and guidance," Twitter said.

"In spite of these challenges we will continue to aggressively enforce our rules in this area and engage with authorities and other relevant organizations to find viable solutions to eradicate terrorist content from the Internet and promote powerful counter-speech narratives."

Pressure has been growing on social networks since attacks in

Paris in November and southern California in December which were linked to supporters of the Islamic State group, sometimes referred to as ISIS.

The White House last year called for "dialogue" with Silicon Valley and others on the subject, saying more should be done "when the use of social media crosses the line between communication and active terrorist plotting."

The European Commission has also called for talks with major social media networks. And France passed emergency measures last year that could shut down websites or social media accounts which encourage terrorist actions.

In Congress, Senators Dianne Feinstein and Richard Burr proposed legislation to require online communications services to report potential terrorist activity.

Twitter said it has long sought to enforce its rules on promoting violence, while maintaining an open platform.

"As an open platform for expression, we have always sought to strike a balance between the enforcement of our own Twitter rules covering prohibited behaviors, the legitimate needs of law enforcement, and the ability of users to share their views freely - including views that some people may disagree with or find offensive," the blog said.

But in recent months, Twitter added that "we have increased the size of the teams that review reports, reducing our response time significantly" and used "spam-fighting tools to surface other potentially violating accounts for review by our agents."

By ramping up the efforts, Twitter said, "we have already seen results, including an increase in account suspensions and this type of activity shifting off of Twitter."

Last March, Facebook updated its "community standards," saying this would curb the use of the social network giant for promoting terrorism or hate speech.

The update said Facebook will not allow a presence from groups advocating "terrorist activity, organized criminal activity or promoting hate."

The move came after videos of gruesome executions appeared on Facebook and other social media as part of Islamic State group propaganda efforts.

Facebook Is Handing Out $1,000 Credits If You Want To Run Advertisements Against ISIS

Washington, D.C. is pleading with Silicon Valley to figure out some way to fight ISIS online. So companies like Facebook and Google are bringing out the biggest guns the modern tech sector has: megalithic, all-seeing advertising platforms.

Facebook is giving away $1,000 credits to groups that want to run advertisements showing anti-ISIS propaganda, the Wall Street Journal reports.

Social media is an essential element of jihadist recruitment in the West, and Facebook has spent months developing its anti-ISIS strategy. In one case, it let some jihadis make accounts and then struck up long-lasting conversations with them. Last fall, Facebook held competitions with 45 colleges, awarding thousands of ad dollars to student teams running anti-jihadist messages.

Hearts and likes campaign: Facebook’s new anti-ISIS effort comes after similar declarations from other major internet companies. Twitter recently broke its silence on the issue of ISIS accounts to announce that it has banned tens of thousands of ISIS handles, and Google announced a nearly identical program earlier this month, giving free ad placement to people who run anti-ISIS propaganda campaigns possibly Facebook’s inspiration for publicizing its own program.

"This year ... we are running two pilot programs," Google executive Anthony House told a committee of the U.K. Parliament. "One is to make sure these types of views are more discoverable. The other is to make sure when people put potentially damaging search terms into our search engine, they also find these counter-narratives."

"Right now it’s an assumption [based on thinking that] better ideas ultimately defeat worse ideas."

But even if government entities and NGO’s reach as far as Hollywood to find someone to produce effective, enlightening messages that encourage people to turn people away from terror, counterterrorism experts aren’t sure that uplifting anti-propaganda actually works.

"Right now it’s an assumption [based on thinking that] better ideas ultimately defeat worse ideas," William Braniff, executive director of the National Consortium for the Study of Terrorism and Responses to Terrorism, told the Journal.

Still, some people are convinced that likes, shares and maybe even a few pokes can help stop ISIS’s influence in the West, even if those people are mostly Facebook employees.

Hackers Get Employee Records at Justice and Homeland Security Depts.

In the latest cyberattack targeting the federal government, an intruder gained access to information for thousands of employees at the Justice Department and the Department of Homeland Security, but officials said Monday that there was no indication that sensitive information had been stolen.

Most of the information appeared to have been culled from internal government directories, including employees email addresses, phone numbers and job titles.

Motherboard, a technology news site, reported on Sunday that it had been approached by a hacker who claimed to have obtained employee information on about 20,000 people at the F.B.I. and 9,000 at the Department of Homeland Security.

The hacker professed support for pro-Palestinian groups and vowed to make the information public in an apparent attempt to embarrass federal agencies that play a part in cybersecurity operations. The hacker released the information on Sunday and Monday.

Officials at the Justice Department and the Department of Homeland Security said they were examining the breach.

There is no indication at this time that there is any breach of personally identifiable information, said Peter Carr, a spokesman for the Justice Department. Marsha Catron, a Homeland Security spokeswoman, echoed that statement.

It was unclear when the breach had occurred or whether it was connected to an intrusion last fall that exposed personal emails of Jeh Johnson, the Homeland Security secretary, and John O. Brennan, the C.I.A. director. The hackers who claimed to have carried out those attacks also expressed pro-Palestinian views.

The new breach does not appear to have resulted from an attack using an outside computer to penetrate the system. Instead, officials said, they believe that the intruder impersonated a government employee and used that information to get into other parts of the system.

The officials would not elaborate on how that had been done, but they described it as a social engineering breach, which could involve pulling personal information from social media and using it to determine a user s passwords.

Agencies across the federal government have struggled to keep computer information secure from both outside hackers and their own employees.

A much bigger intrusion that targeted the Office of Personnel Management exposed security clearance dossiers and sensitive information for nearly 22 million Americans. Chinese hackers were thought to have been behind the attack, which was much more sweeping than officials publicly acknowledged last year at the outset.

Vigilante Hackers Aim To Hijack 200,000 Routers To Make Them More Secure

The same "Vigilante-style Hacker," who previously hacked more than 10,000 routers to make them more secure, has once again made headlines by compromising more than 70,000 home routers and apparently forcing their owners to make them secure against flaws and weak passwords.

Just like the infamous hacking group Lizard Squad, the group of white hat hackers, dubbed the White Team, is building up a sizeable botnet consisting of hundreds of thousands of home routers, but for

a good purpose.

Lizard Squad, the same group responsible for Sony PlayStation Network and Microsoft Xbox Live outages, uses their botnets to launch DDoS (Distributed Denial of Service) attacks against target websites to flood them with traffic and knock them offline.

Challenged by Lizard Squad’s maliocus work, the White Team of vigilante hackers built their own peer-to-peer botnet that infects routers to close off vulnerabilities, such as:

- Weak default passwords
- DNS poisoning
- Unauthorised access (backdoor)
- Disabled firewalls

Their malware, dubbed "Linux.Wifatch" a.k.a "Wifatch" that has been used by the team since last year continues to be updated and has been open-sourced on Github.

The malware, first discovered in November 2014 by an independent malware researcher "Loot Myself" and analysed by Symantec last year, now includes more programs to remove other malicious software and backdoors already on the system.

The White Team has access to around 70,000 devices, according to Symantec, who is continuously watching over the team’s botnet.

Lizard Squad sizable botnet contained somewhere between 120,000 and 150,000 bots, a Lizard spokesperson told Forbes, claiming that their botnet includes not just home routers and PCs, but smart refrigerators, smart TVs and other smart home devices as well.

The White Team aims at hacking and protecting between 150,000 and 200,000 devices from Lizard Squad attacks, thereby removing the rogue gang from people’s homes.

However, the team of vigilante hackers face some hurdles, especially when working with the Wifatch malware, which is often too big to install on smaller routers.

"The goal is to use (most) of the 60,000 nodes we have to connect to the hundreds of thousands of boxes that are too small for our normal disinfector and disinfect them remotely," the hacker collective told the publication over encrypted email.

Since there are so many vulnerable devices that can be hacked with little or no effort, these vigilante hackers aren’t answer to this widespread problem. They can only help minimize the issue.

The White Team is not the only team of vigilante hackers trying to secure the Internet. Just last week, a hacker replaced a malware with antivirus software. An anonymous hacker was found replacing Dridex, the most active banking malware, with the copies of Avira security software.

Apple Hired the Hackers Who Created the First Mac Firmware Virus

Apple has hired two security researchers who previously worked on viruses targeting Mac computers.

LegbaCore founder Xeno Kovah revealed on Twitter in November that he and his partner, Corey Kellenberg, had been hired by Apple to do low level security. The move went unnoticed until another security researcher revealed it during a presentation at a security conference in December.

LegbaCore was best known for developing a proof-of-concept virus-worm hybrid called Thunderstrike 2 that targeted Mac computers. The worm that Kovah developed was able to spread from MacBook to MacBook, even if the computers were not connected to the internet.

 [The attack is] really hard to detect, it s really hard to get rid of, and it s really hard to protect against something that s running inside the firmware, Kovah told Wired in July.

Kovah s worm virus was the first to attack Macs at the firmware level, according to Wired, which means it targeted the software that boots up before the computer s primary operating system, OS X. It s a valuable kind of attack because it usually can t be detected by antivirus and other security software.

After Thunderstrike 2 installed itself on a target s computer, it could spread to certain peripherals, such as a Apple-branded Thunderbolt Ethernet adapter, which would then spread the virus to other Macs it was plugged into.

But instead of exploiting their findings or selling it to the highest bidder, Kovah and team notified Apple of the vulnerabilities, which have since been fully patched. Although Apple does not pay bug bounties to researchers for finding security problems, the high road seems to have worked out for the founders of LegbaCore.

All 160 Million eBay Users Can Be Hacked: Fake Sales Listings Make Users Vulnerable To Infection

A security vulnerability on eBay could enable hackers to embed malicious code and target buyers and sellers on the popular auction website. The flaw, which remains unpatched, could also make it possible for hackers to send out phishing links containing the malicious code, tricking recipients into believing an infected email was sent by eBay.

Researchers at the Israeli cybersecurity company Check Point first found the bug last year, quietly disclosing the vulnerability to eBay Dec. 15. The company responded Jan. 16 although it still has yet to provide a fix nearly two months after the initial disclosure, the software news site PCI News reported Thursday.

The vulnerability makes it possible for attackers to subvert eBay’s code validation (which is meant to filter out any illegitimate data transfers) and inject malicious JavaScript code. The attack takes place when users are directed to what appears to be a shopping website that actually contains the malicious JavaScript code. From there, the code scans a user’s computer for personally identifiable information or unwittingly enlists the machine in a botnet army (used to launch distributed denial-of-service attacks).

All of eBay’s 160 million users could become victims in the attack, Israel’s Channel 2 News reported.

The eBay attack flow provides cybercriminals with a very easy way to target users: sending a link to an attractive product to execute the attack, Oded Vanunu, security research group manager at Check Point, said in a blog post. The main threat is spreading malware and stealing private information. Another threat is that an attacker could have an alternate login option pop up via Gmail or Facebook and hijack the user’s account.

This security disclosure comes after more than 100 sales listings were set up as bait to dupe customers into turning over personal information in September 2014, the BBC reported. Smartphones, televisions and other attractive items were listed for sale to direct customers to the fake page where they were asked to log in with their eBay credentials and share banking information. The e-commerce company was heavily criticized after it released a statement saying it would not suspend use of JavaScript or Flash, the software that made the attack possible.

Obviously having JavaScript and Flash and all that wonderful stuff is great for the seller, security researcher Brian Honan told the BBC. But is exposes eBay and its customers to security risks. Until eBay has the ability to automatically identify malicious links, it should disable JavaScript until they have some way of better controlling the risk. The needs of the many outweigh the needs of the few.

Anti-piracy Group BREIN Demands Torrents Time Cease and Desist

Not even a week has gone by since Torrents Time appeared on the scene, and the site has already been served with a cease-and-desist letter. Anti-piracy group BREIN, based in the Netherlands, has deemed the streaming tool an illegal application and demands the administrators cease and desist the distribution of Torrents Time immediately.

Torrents Time provides an embedded torrent client that lets users download and play the files inside torrents with one click. There is no need to download and install a separate BitTorrent client, download and open the torrent, or go in and actually play the download video file. After you install the plugin, everything happens in the browser. Torrent sites, including notorious The Pirate Bay, have very quickly adopted the solution.

Here is the crux of BREIN s complaint:

Through your website Torrents Time (https://torrents-time.com/) you are distributing the illegal application Torrents Time that structurally and systematically facilitates, enables and participates in the making available of infringing content without the authorization of the respective copyright and neighbouring rights holders. Torrents Time is enabling the illegal distribution of popular titles of films and of TV-Series that are published by the rights holders represented by BREIN and which have not been licensed for distribution through your system.

The group argues that because Torrents Time is hosted on servers located in the Netherlands, the country s law applies to Torrents Time, which BREIN further describes as primarily engaged in the facilitating, enabling and participating in the making available of infringing files. The key word here is primarily as of course Torrents Time, like any BitTorrent client, can be used to obtain torrents that do not contain pirated content. BREIN adds that the tool causes extensive damage to rights holders for which you and all others involved with the management of the site are liable.

In addition to the cease and desist, the anti-piracy group also requests the geographical address of yourself and the entity or other person(s) who are responsible for the distribution of Torrents Time. The reason? So that BREIN can hold Torrents Time liable in case you continue your unlawful activities. If Torrents Time does not comply, BREIN will request that the site s host take down the site and provide it with the administrators names and addresses. Oh, and BREIN will hold Torrents Time liable for all (further) incurred costs including legal fees.

Torrents Time isn t playing ball. The administrators have responded with their own letter, and the tone is very dismissive. Here is the introduction:

From the outset, please be informed that my clients deny all the suppositions and assumptions in your letter, including the fact that Brein represents right holders and that you are qualified to take action on behalf of an un-named un-identified entities. That having been said, your allegations as to the legal nature of my Clients are certainly denied as frivolous and without substantiation. In your letter, you take the liberty of accusing my Clients of distributing an illegal application. We deny that allegation, as being un-substantiated, false and illegal in itself, under the laws of the Netherlands.

Torrents Time is countering with the simple fact that its tool can be used to watch legally obtained videos. Indeed, the Torrents Time website in itself does not let users stream pirated content.

The response letter further goes on to point out that no court has ever ruled that Torrents Time breaches copyrights nor neighboring rights because the tool was released just a few days ago and was carefully crafted not to do anything whatsoever so as to breach copyright or neighboring rights. The lawyer also states, I am confident that the outcome of a court proceeding against my Clients Torrent Time will end with a ruling against anyone who challenges the legality of Torrents Time.

The letter then attempts to go on the offensive:

> You are therefore advised to seriously re-think your cease and desist demand and advise my Clients that you withdraw your demands. You are also hereby warned not to attempt to take action against any third party who utilizes Torrents Time or hosts it or co-operates therewith in any other manner. Failing to comply with my demands herein will prove itself as enormously costly to your organization and its members and could lead to criminal proceedings against yourself, on the grounds of illegal threats and extortion, the consequences of which I m sure you are very well aware of.
>
> In the circumstances, and in order not to incur un-necessary legal bills, I advised my Clients to send you a draft of my letter, unsigned, so as to stop the fight before it becomes unstoppable. Please do not take this gesture as a sign of weakness but as a good faith action. We are, like yourself, professionals very well versed with the subject matter at hands, for more than 3 decades. We hope that you are a member of the legitimately acting legal society and not a mob thug.

Torrents Time is growing quickly, and the administrators are eager to provide commentary. Indeed, this is how we found out about the BREIN cease and desist.

> We launched last week and in a few days changed forever the way people use the treasures found through torrents sites, directly from their browser, Torrents Time told VentureBeat. It means that from today on, any user who is able to use Facebook can enjoy almost any movie or TV show that was created in this world. Torrents Time is revolutionizing the world of torrents, here and now. Because it s a revolution, you can expect a bloodshed, like the fate of all revolutions. We already managed to get a cease and desist letter from BREIN.

It would appear Torrents Time is almost proud to receive the cease-and-desist letter. The administrators were certainly expecting one, though maybe not in the same week they released the tool. Their whole demeanor is very confident this is a fight they believe is an inevitable win.

> But because it s the people s revolution, a network of hundreds of millions of people who wish to consume Free Content, the people will prevail and the illegal harassment by the film and TV producers industry who claim that p2p ruins their business model will be defeated, the administrators added. With p2p we make the world smaller, a people s village where all the neighbors can watch together the staff they like. Freely! Like they watch YouTube together or share content on Facebook.

And again they reiterate that this is not about piracy: Torrents Time is not a pirate s tool. It s cool and it s legal. We are certain it will improve the world.

BREIN and other groups naturally disagree and will be doing everything in their power to stop Torrents Time from taking off. But the streaming solution is already out there, and even if they could, wiping the Torrents Time team off the face of the Earth wouldn t help.

You can t put the genie back in the bottle.

Internet of Things Might Be Used for Spying

If you re reading this online, then there s a chance that someone could be spying on you.

James Clapper, the U.S. Intelligence Chief, admitted that certain security agencies in the near future could use smart devices for surveillance, identification and tracking. Although this isn t a total shocker when you consider how openly we share our information online, it still makes you feel a little uneasy.

The Internet of Things is the network composed of physical devices that connect and share data with one another. It s the unseen line of communication that lets you send an email from your computer to your phone. For example in some modern homes like this one, you can control your high tech garage door from your phone, while at the same time have your refrigerator send you a reminder that you need to stock up on eggs.

A study from Harvard University indicates that many home appliances have wireless sensors that all connect to the Internet of Things. Even appliances like toasters, bed sheets and toothbrushes could have a sensor that collects data about you.

Clapper stated that these agencies are using the Internet of Things for their spying. This means that your devices are not secure, and your privacy is not guaranteed.

Take a look around your house. Your TV, laptop and cameras could be sending a live video feed to someone right now.

About a year ago, people were nervous because it was reported that the new Samsung Smart TV always had its microphone on. The reason for this was so you could get it to turn on with a simple voice command, but this feature rightfully freaked out people because it meant someone could always be listening to what you were saying.

Another unnerving security story came a few years ago when someone hacked into a baby monitor in the middle of the night and started screaming at the baby. The hacker got access to the device through the wireless IP network and could see and hear what was going on in the house. This is why you should always be careful and understand the technology you are buying before you purchase it.

Other devices like your Fitbit, Apple Watch and Amazon Echo could be used to listen to your conversations, look into your house or monitor your health. This just goes to show how easily the U.S. government might be able to spy on you by simply using devices that have become of part of your everyday life.

Some of these devices are a necessity in our culture and will be hard to stop using, so what can you do to protect yourself? If you are using your technology safely and have a secure wireless connection, you ll have a better shot at preventing unwanted

access to your devices and your life.

13 Essential Rules for Staying Safe on the Internet

Feb. 9 was Safer Internet Day. For the past 13 years, cyber-advocates across the world have used the second Tuesday in February to remind people to be careful out there. The day is now observed in more than 120 countries. And while most of the discussion is focused on keeping kids out of harm s way, adults can also learn a thing or two.

Internet safety is also about securing yourself from cybercriminals, snoops, creeps, and assorted other denizens of the Net s dark side. Follow these 13 rules and you should be able to surf in safety.

Rule #1: Update early and often

If there s a vulnerability in your operating system, browser, or other software, be assured the bad guys know about it. But no matter how quickly software makers plug that hole and push out an update, it won t do a damn bit of good if you don t actually install it. So install updates as soon as they re available, especially those marked critical. Better yet, set your OS and apps to automatically update if possible. Yes, it s a hassle to update Java and Adobe Acrobat every flipping week, and some updates may occasionally break things. Do it anyway.

Rule #2: Honor thy antivirus software and keep it current

Installing antivirus software isn t the safety net it used to be, thanks to the increase in zero day threats that appear before AV companies can update their software. But they ll still stop more than 90 percent of the threats you re likely to encounter. So get some. If you re unwilling to pony up $30 to $60 a year for BitDefender or Intel s McAfee, you can download perfectly adequate solutions from AVG or Avast for free.

Rule #3: Don t fall for that scam

You know what s an even bigger threat than malware authors and cybercrooks? You. The easiest way for an attacker to get access to your logins is to fool you into giving them up. This is usually achieved via a phishing email that looks like it s from your bank, employer, or the IRS; this email aims to lure you to a bogus site where you enter your login name and password. Once the attackers have your info, they can log into your account, then steal your information and sell it to others.

Some phishing attempts are crude and easy to spot; others would fool all but an expert. But the defense is easy: Just don t click on any links inside an email. If you got an email purportedly from your bank, type your bank s web address into the browser and go there directly.

Rule #4: Don t touch that file

The other way scammers get you is by sending a bogus attachment, like an invoice or a contract for something you allegedly ordered. Opening the document usually infects your computer. If you don t recognize the sender, just delete the email. If the message appears to come from a friend or colleague, make triple sure that person actually sent it to you before you open it.

Rule #5: Become a cyber-savvy parent

Sexting, cyberbullies, and catfishing being a parent of an Internet-age kid isn t easy. The best thing you can do is educate yourself. The Connect Safely site has a slew of helpful, nonhysterical guides to keeping kids safe from cyberbullies, dealing with SnapChat and Instagram, how to handle the mobile phone conundrum, and a ton more. Common Sense Media is also an excellent resource for how to be cyberparent, with recommendations for age-appropriate sites, apps, games, and the like.

Rule #6: Don t be a boob about the Tubes

If your kids are online, it s pretty certain they re spending a lot of time on YouTube and other video sites. Most of that content is innocent (if mind-numbing); some of it isn t. You need to at least be aware of what they re watching and put some controls on it. If they re still in single digits, you might want to install Google s YouTube Kids app on their tablets or phones.

Rule #7: Don t install that new video player

Just like in real life, most of the bad guys on the Internet hang out in dicey neighborhoods like adult sites, BitTorrent search engines, and pirate Internet TV stations. At some point nearly all of them will pop up a message saying that your Flash player is out of date or that you need to install a new video player to watch whatever it is you re trying to watch. Don t do that.

This pirate site wants me to update Flash, but it s really trying to get me to install malware. (Also: Don t use Flash if you can avoid it.)

Best-case scenario is you ve installed adware software that will splatter advertisements over all your Web pages. Worst case, somebody just made your computer part of their zombie army.

Rule #8: Use a password manager

Yes, passwords suck. But until we get a better replacement, we re stuck with them. So do yourself a favor and use a password manager like 1Password, Dashlane, or Lastpass. They will both act as a password vault, storing all your thousands of logins for different sites, and also auto-generate fiendishly difficult-to-crack passwords on your behalf. Just don t forget the master password to your vault or you re screwed. (Tip: Use a song lyric or some other easy-to-remember-yet-unique phrase for your password, the longer the better.) They aren t foolproof, but they re better than using 123456 for everything.

Rule #9: Protect your logins

One way to find out if your password has been stolen is to see if

someone is logging into your accounts from an unknown machine. With more and more sites using Facebook and Twitter as ways to prove you are who you say you are, this becomes especially more important.

Facebook has a Security Checkup page you can use to see if someone else has been logging into your Facebook account and lets you log out of any unknown ones with a click. Companies like Apple, Google, Twitter, and Yahoo have deployed so-called two-factor (or two-step) authentication, which requires you to enter an additional piece of information when logging in from an unfamiliar device usually a 4- or 6-digit code sent via text to your phone. If you think someone else might have access to your accounts, it s a good idea to change your password and then implement two-factor.

Rule #10: Secure all your Wi-Fi passwords

Most people don t realize this, but your home Wi-Fi actually has two passwords. One is for the network that s the one you type when you log on from a new device. The other password is for the router; this allows you to go in and change network settings (like your Wi-Fi password). Most people remember to change the first set of logins but not the second, and the router defaults are widely known (usually admin and password). So anyone within range of your home network could log into your router, change the settings, lock you out of it if they wanted to, or simply capture all the information flowing out of your network. Not good.

You ll want to change your router s defaults. Instructions vary depending on the router, so you ll need to visit the manufacturer s website and search for change router admin password. (To get you started, here are instructions for Netgear, Linksys, and Belkin.)

Rule #11: Don t get sucked in by fake Wi-Fi hotspots

If you re logging on from a crowded cafØ or an airport lounge, you ll probably see free Wi-Fi hotspots galore. Some are legit, some are definitely bogus. You ll want to find out if in fact the cafØ or lounge offers free Wi-Fi, and what the network name is, before you log on. Otherwise you could be handing all your Internet traffic to some rogue access point or that creep behind you with a laptop. When in doubt, pony up some money for a legit public hotspot you know is secure.

Rule #12: Use an encrypted connection in public

Even if you re on a legit public Wi-Fi network, someone else on the same network could snoop on your data unless you take the right precautions. First, if you are logging on to your webmail or another password-protected account, make sure to use the encrypted version of the website the address always starts with https (not http). Otherwise, anything you type is sent in plain text and can be captured by someone else on the same network.

A good explanation of how two-step authentication works, courtesy of Google.

The best option, if you can: Connect to the Internet using a virtual private network (VPN), especially if you re dialing into work. This creates an end-to-end encrypted connection between you

and the Net, making it virtually impossible for anyone to spy on you.

Rule #13: Technology can help but it can t solve everything

If you ve got kids at home, technology can give you a handle on what they re doing on the Net. Circle can monitor every device on your home network and let you set rules about where and when kids can access the Net. (Unfortunately, right now it works only on iPhones; Android support is coming later this year.) The upcoming Screen app will let you control all your home devices from your phone. Norton Online Family Premier can cordon off the nastier parts of the Net and give you a window into their chat conversations and video consumption. And of course, anti-malware software can help fight off the nasties for everyone.

Ultimately, though, the burden is on you. Like liberty, the price of Internet safety is eternal vigilance. And not just on one day each year.

Obama Says Passwords Aren t Strong Enough, Urges Use of 2FA

President Obama says that we re right: passwords aren t enough.

We need two-factor authentication (2FA) to protect ourselves online, he said on Tuesday in an editorial in the Wall Street Journal.

Granted, he didn t mention Naked Security per se, but he did announce a slate of federal initiatives to improve the nation s information security.

That includes a new national awareness campaign to get Americans to do what security people keep urging them to do: use 2FA whenever possible.

From his editorial:

> [W]e re doing more to help empower Americans to protect themselves online. In partnership with industry, we re launching a new national awareness campaign to raise awareness of cyberthreats and encourage more Americans to move beyond passwords adding an extra layer of security like a fingerprint or codes sent to your cellphone.

The op-ed coincided with the release of a broad cybersecurity plan that proposes boosting federal cybersecurity spending by more than a third, to over $19 billion.

The White House is so intent on improving the country s security that it s going to woo Silicon Valley types, the president said relaxed business attire and all:

> [W]e re stepping up our efforts to build a corps of cyber professionals across government to push best practices at every level. We ll do more including offering scholarships and forgiving student loans to recruit the best talent from Silicon

Valley and across the private sector. We ll even let them wear jeans to the office.

The president also issued an executive order to create a new Federal Privacy Council: an interagency forum to improve the privacy practices of government agencies and entities acting on their behalf.

They sure do seem to need it.

The same day that the president s editorial ran, news broke about a PIN-stealing attack on the e-filing app on IRS.gov, the site of the Internal Revenue Service (IRS).

The attack, carried out last month by an automated bot, affected 101,000 taxpayers.

As Naked Security s Paul Ducklin noted, the attack was ironic in that it involved a sort-of, not-really form of 2FA.

The e-filing PIN is a type of second authentication factor needed for 2FA.

You need the PIN, along with other personal data, when submitting online tax returns.

But that s not exactly how 2FA s supposed to work, in that you shouldn t be able to request one of your factors by using the other factor.

The way 2FA should work is that you need to prove yourself in two different ways before you can log in or use a service.

For example, in order to withdraw money from an ATM, just inserting your card (your first factor) isn t enough. You also need to enter a second factor   your PIN.

The IRS actually offers a special, stronger form of 2FA, known as the IP Identity Protection PIN (IP PIN).

But for whatever reason, the IRS doesn t hand out an IP PIN to just anybody.

Rather, it s only available to taxpayers who ve already suffered some kind of identity breach.

Other things in the president s plan:

A proposed $3 billion fund to overhaul dusty old federal computer systems. As it is, government IT is like an Atari game in an Xbox world, President Obama said. The Social Security Administration uses systems and code from the 1960s. No successful business could operate this way.

Creation of a new federal infosec position. The title will be Chief Information Security Officer.

A new cybersecurity Center of Excellence. It will bring together industry and government experts to research and develop new cutting-edge cyber technologies, Obama said.

A national testing lab. Companies will be able to test their systems security under simulated attacks.

Training for small businesses. The training, offered by the Small Business Administration, will be available to over 1.4 million small businesses and their workers, the president said.

We re cheered by the president s backing of 2FA.

It s an acknowledgement that passwords are often the weakest link in authenticating that users are who they say they are.

As the yearly lists of the top bad passwords show, many don t use passwords that are complex enough.

Others reuse passwords, setting themselves up for account break-ins when online crooks acquire logins from breaches or third-party sites, such as happened last month to Fitbit.

Even complex passwords can be susceptible to brute-force attack: we saw that when researchers recently managed to pry 18,000 Bitcoiners passwords out of their wallets, running the attack off a mere $55 worth of Amazon Server.

2FA can help.

Hopefully, so too can blue jeans-clad Silicon Valley types: the kind of people who can do things like convince the IRS to proactively hand out strong 2FA like the IP PINs to all who ask, not just to those who ve already suffered identity theft and/or tax fraud.

Malware Museum Lets You Safely Experience The PC Viruses of Yesteryear

We re all familiar with malware as an insidious menace that seeks to steal your personal information and ransom your data, but it was not always so. In the early days of personal computing, viruses were less of a malicious threat and more of an annoying joke. Now you can relive the glory days of mostly harmless computer viruses by visiting the Malware Museum hosted at the Internet Archive.

The collection consists of a few dozen examples of early malware curated by computer security expert and researcher Mikko Hyppönen. All the examples of antique malware in the museum are from the 80s and 90s, and will run entirely in your browser using a DOSBox emulator. That keeps you nice and safe, but the original files have also been cleansed of dangerous code. You can download the modified files if you want to play around with them on your own system.

Just a few minutes in the Malware Museum will drive home how different things used to be. Many of the viruses hosted are hardly malware they re more or less neutral. Modern malware is usually designed with a financial incentive in mind, so limiting detection is an important aspect of the payload. If the user doesn t know the virus is there, they won t know to get rid of it. These classic viruses were all about making sure the user knew they had been hacked. It was about the prestige of making something clever and interesting.

Some of the examples in the Malware Museum do little more than display a fun graphic on the affected computer. For instance, the Q Walker virus causes a character from the Commodore 64 game Bop n Rumble to stroll across your screen (see below). He just keeps doing it, though, which I assume would be annoying. Then there s the Mars G virus, which notes as it loads that coding a virus can be creative. This one generates a moving Martian landscape using voxel rendering. It doesn t even stop you from using the computer as you can hit any key to exit.

There are, however, genuinely malicious pieces of software from this era that will be much more familiar to modern computer users. There s the Casino virus, which existed solely to ruin people s days. When it was loaded onto a system, it would delete the file allocation table (FAT) on the disk, thus making important files inaccessible. However, it offered victims a possible recourse by winning a slot machine game. You have five tries to hit the jackpot, and winners will have the FAT restored from RAM. It s a bit like modern ransomware, except without the actual ransom.

The Malware Museum has attracted more than 100,000 visitors since it went up last week. That has to be a record for people visiting a page specifically because it hosts viruses.

Bye Bye, Flash! Google To Ban Flash-based Advertising

Google had also joined the path of Apple, Facebook, and Youtube to kill the "Adobe Flash Player" by announcing that the company is banning Flash banner support from its Adwords Advertising platform.

"To enhance the browsing experience for more people on more devices, the Google Display Network and DoubleClick Digital Marketing are now going 100% HTML5" Google says.

It’s been two decades since Adobe Flash has ruled the Web Space Animation Arena, which was the de facto standard for playing the online videos.

Flash Player had been famous for Zero-day exploits which are a potential threat to online users.

Even Adobe tried to maintain equilibrium by releasing a countless number of patches frequently (that got hiked), for instant reported vulnerabilities, but this had annoyed both customers and companies.

The endless troubleshooting of the Flash Player plugins never resolved the vulnerabilities.

To put a full stop on this issue... many major tech companies like Apple, Facebook, Youtube, Google Chrome, Firefox had been magnetized towards the new substitutor - HTML 5.

Facebook’s Security Chief publicly called for Adobe to announce a ’kill-date for Flash.’
Google Chrome has also begun blocking auto-playing Flash ads by

default.
In January this year, YouTube moved away from Flash for delivering videos.
Firefox also blocked the Flash plugin entirely.

By ending up Flash, all the above companies found a silver bullet to the security issues that have plagued Adobe Flash for years, as well as eliminated a third party dependency.

Steve Jobs was right about the end of Flash as he quoted as saying in his letter:

New open standards created in the mobile era, such as HTML5, will win on mobile devices (and PCs too). Perhaps Adobe should focus more on creating great HTML5 tools for the future, and less on criticizing Apple for leaving the past behind.

HTML 5 has gained a Word of Mouth Popularity by many developers and also have many advantages like to play the video smoothly, in fact, in a better way.

So, Google also officially declared that it would not support Flash ads in Doubleclick Digital Marketing from July 30, 2016.

Moreover, from January 2, 2017, the company will discontinue the support for Google Display Network as a part of complete Flash Wipe Out.

However, as a Result of this awful reputation, Flash Player would be rebranded as Animate CC with some additional features like the direct conversion of Flash Files to HTML5 Canvas files.

Adobe Animate CC mostly looks like an update to the Flash Professional software supports Adobe Flash (SWF) and AIR formats 'as first-class citizens,' along with other animation and video formats, including HTML5 canvas, 4K and WebGL output.

Windows 10 Sends Your Data 5500 Times Every Day Even After Tweaking Privacy Settings

Myth: By disabling all privacy compromising and telemetry features on Windows 10 will stop Microsoft to track your activities.

Fact: Even after all telemetry features disabled, Windows 10 is phoning home more than you could ever think of.

Ever since the launch of Microsoft's newest operating system, Windows 10 is believed to be spying on its users. I wrote a number of articles to raise concern about Windows 10 privacy issues, including its controversial data mining features and privacy invasion features.

The only solution believed to cope up with these issues is to disable all the telemetry features or use an automated tool to disable all privacy-infringing features in just one click.

But unfortunately, all these efforts got wasted because Microsoft

still tracks you, even after you tighten your Windows 10 privacy to an extreme level, claims the recent analysis conducted by a Voat user CheesusCrust.

Curious to know the extent of Windows 10 spying, CheesusCrust set up his Linux laptop with a Windows 10 Enterprise virtual machine as well as a DD-WRT router that was being utilized to monitor traffic.

CheesusCrust also disabled every single tracking and telemetry features in the operating system. He then left the machine running Windows 10 overnight in an effort to monitor the connections the OS is attempting to make.

The results are not so surprising:

Eight hours later, he found that the idle Windows 10 box had tried over 5,500 connections to 93 different IP addresses, out of which almost 4,000 were made to 51 different IP addresses belonging to Microsoft.

After leaving the machine for 30 hours, Windows 10 expanded that connection to 113 non-private IP addresses, potentially allowing hackers to intercept this data.

Taking his test to a step further, CheesusCrust again installed Windows 10 Enterprise virtual machine on his laptop, disabled all tracking features and enabled a third-party tool known as DisableWinTracking.

After this, the number was reduced to 2758 connections to 30 different IP addresses in the period of 30 hours.

The interesting fact here is: This analysis was conducted on Windows 10 Enterprise Edition that comes with the most granular level of user control, far more than the standard Windows 10 Home Edition used by a sizable audience.

However, based on these logs, it would be inaccurate to say that Windows 10 is sending your personal data to Microsoft’s servers. But, thousands of connection attempts in the period of 8 hours just to check for updates or adjust the time, sounds more complicated than thought.

A September 2015 blog from Terry Myerson, head of the Windows team, explained that while Windows 10 does send some of your data to the company, everything is encrypted and doesn’t include any of your personal details.

Here’s what Microsoft says about the Windows 10 Spying concerns:

"We collect a limited amount of information to help us provide a secure and reliable experience. This includes data like an anonymous device ID, device type, and application crash data which Microsoft and our developer partners use to continuously improve application reliability. This doesn’t include any of your content or files, and we take several steps to avoid collecting any information that directly identifies you, such as your name, email address or account ID."

While this research doesn’t provide what details Windows 10 is sending to the company even after disabling the telemetry features, you have to keep this in mind that Nothing comes for FREE. "Free" is just a relative term. May be you are paying the greatest cost to owning Windows 10.

Wired to Ad Blocker Users: Pay Up for Ad-free Site Or You Get Nothing

Wired readers who use ad blockers, you ve been warned.

Soon you won t be able to get any online content from the popular tech publication unless you stop blocking their ads, or pay for the privilege of seeing no ads.

For a while, if you visited Wired.com with an ad blocker enabled, you were presented with a message politely asking you to support the publication by disabling your ad blocker or whitelisting the site.

That message (ironically, featured in a display ad), has now been replaced with an ad announcing that Wired will soon be launching an ad-free version of the site, for which you have to pay a subscription.

In a note titled How Wired is going to handle ad blocking, Wired s editors plead their case that ad blockers are undercutting the revenues that pay for the publication:

> We know that you come to our site primarily to read our content, but it s important to be clear that advertising is how we keep WIRED going: paying the writers, editors, designers, engineers, and all the other staff that work so hard to create the stories you read and watch here.

Unlike some ad blocker critics in the advertising and publishing industries, Wired acknowledges the legitimate reasons why so many millions of people (and 20% of Wired.com visitors) use ad blockers: blocking ads generally means a faster and less annoying web browsing experience, and cuts down on substantial security and privacy risks.

No, you re not causing the demise of the publishing industry if you use an ad blocker, but this stuff isn t free, the editors seem to be saying.

If you want to continue to read content from Wired, you have only two options: disable your ad blocker when you visit the site, or pay for the ad-free version of the website.

If you don t disable your ad blocker, or pay for the ad free site, you re out of luck you won t get to see any Wired content.

By disabling your ad blocker on the site, Wired says you ll only see polite, standard display advertising.

The subscription-based, ad-free version of the site will have no

display advertising and no ad tracking, Wired says.

In a sense, this is what counts as a compromise in the ad-blocker wars.

Instead of using anti-ad-blocking technology to ignore the wishes of users who want to block ads and serve them ads anyway, Wired is giving its readers a choice albeit one that ad blocker users probably won t like.

Wired says it will continue to experiment with ways to publish stories, while also maintaining a healthy business that supports the storytelling.

What that might look like is unclear, but some publishers are getting around ad blockers by blurring the lines between editorial content and advertising with so-called native ads.

Readers at Naked Security have some very strong opinions about ad blockers, and we d like to know if you agree or disagree with Wired s approach.

Would you turn off your ad blocker to use the site with ads? Or pay for a version of the site without ads?

Or would you rather walk away?

Microsoft Edge’s InPrivate Mode Finally Keeps Your Activity Private

Browsing the Web in ’Private Mode’ is not as private as you think.

Microsoft has patched the Private Browsing Leakage bug in its newest Edge browser with the latest update.

When we talk about Browsers, only one thing which does not strike our mind is Internet Explorer or IE.

Even there were some trolls on Internet Explorer (IE) waving over the social medias such as "The best web browser to download other browsers."

In fact, it was justified as everyone downloads a new browser with IE in their newly installed Operating System.

Due to the continual taunts, Microsoft had scrapped the entire IE and made a new browser called "Edge Browser" (Codenamed "Spartan").

Edge was shipped as the default browser (along with IE) with Windows 10 devices and grabbed the attention of many eye pupils as it included all the features that other mainstream browsers have.

In January this year, it was reported that ’InPrivate’ mode of the Edge browser is leaking users’ web browsing data.

The InPrivate mode is nothing but Incognito or private support for Windows 10. It has been found storing your browsing history, cookies and cache in a WebCache file on the system, which could be

found easily.

Precisely here:

\Users\user_name\AppData\Local\Microsoft\Windows\WebCache\WebCacheV01.dat

This issue made users feel a repulsive force again and they instantly switched back to other browsers like Firefox or Chrome as the protocols of private browsing mode was correctly followed.

The reported vulnerability was fixed which was included in the update KB 3135174.

The patch update listed as "Fixed issue with Microsoft Edge browser caching visited URLs while using InPrivate browsing."

In another statement made by Microsoft, the company officially claimed that its Edge Browser is much more secure than any other browsers and does not need the support of any armour like EMET anymore.

Enhanced Mitigation Experience Toolkit (EMET) is a Windows tool that shields against the execution of software vulnerabilities in Windows Environment.

As of now, Windows had buried a security hole, but let’s see what’s more coming from the same family.

=~=~=~=